501P036405U500

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed h this Office.

出願年月日
ate of Application: ２０００年　８月２５日

願番号
plication Number: 特願２０００－２６０８６４

願人
licant (s): ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年１２月２２日

特許庁長官
Commissioner,
Patent Office 及川耕造

【書類名】　特許願
【整理番号】　0000608605
【提出日】　平成12年 8月25日
【あて先】　特許庁長官殿
【国際特許分類】　H04K 1/00
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　市村　元
【特許出願人】
【識別番号】　000002185
【氏名又は名称】　ソニー株式会社
【代表者】　出井　伸之
【代理人】
【識別番号】　100086841
【弁理士】
【氏名又は名称】　脇　篤夫
【代理人】
【識別番号】　100114122
【弁理士】
【氏名又は名称】　鈴木　伸夫
【手数料の表示】
【予納台帳番号】　014650
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9710074

【包括委任状番号】　0007553

【プルーフの要否】　　要

【書類名】　　明細書

【発明の名称】　データ送出装置、データ復号装置、データ送出方法、データ復号方法、伝送システム

【特許請求の範囲】

【請求項１】　一連の連続したデータ列のプログラムを暗号化して送出するデータ送出装置において、

ランダムノイズを発生するランダムノイズ発生手段と、

上記ランダムノイズ発生手段で発生したランダムノイズを上記プログラムの前後に付加する付加手段と、

上記付加手段にてランダムノイズが付加されたプログラムに対して暗号化処理を行う暗号化手段と、

上記暗号化手段により暗号化されたランダムノイズが付加されたプログラムを送出する送出手段と、

を備えたことを特徴とするデータ送出装置。

【請求項２】　上記送出手段は、有線又は無線で接続された他の機器に対して上記プログラムを送出することを特徴とする請求項１に記載のデータ送出装置。

【請求項３】　上記送出手段は、上記プログラムを記録媒体に記録するデータとして送出することを特徴とする請求項１に記載のデータ送出装置。

【請求項４】　上記付加手段で付加するランダムノイズのデータ長は可変長とされていることを特徴とする請求項１に記載のデータ送出装置。

【請求項５】　一連の連続したデータ列の前後にランダムノイズが付加され、暗号化が施されたプログラムを入力して復号するデータ復号装置において、

送出されてきたプログラムを入力する入力手段と、

上記入力手段により入力されたプログラムに対して暗号化を解読する復号処理を行う復号手段と、

上記復号手段で復号されたプログラムの前後に付加されているランダムノイズを除去する除去手段と、

を備えたことを特徴とするデータ復号装置。

【請求項６】　上記入力手段は、有線又は無線で接続された他の機器から送出されてきたプログラムを入力することを特徴とする請求項５に記載のデータ復号装置。

【請求項７】　上記入力手段は、記録媒体から読み出されて送出されてきたプログラムを入力することを特徴とする請求項５に記載のデータ復号装置。

【請求項８】　一連の連続したデータ列のプログラムの前後にランダムノイズを付加し、

ランダムノイズが付加されたプログラムに対して暗号化処理を行ない、

暗号化されたランダムノイズが付加されたプログラムを送出することを特徴とするデータ送出方法。

【請求項９】　プログラムの前後に付加するランダムノイズのデータ長は可変長とされていることを特徴とする請求項８に記載のデータ送出方法。

【請求項１０】　一連の連続したデータ列の前後にランダムノイズが付加され、暗号化が施されたプログラムを入力し、

入力されたプログラムに対して暗号化を解読する復号処理を行ない、

復号されたプログラムの前後に付加されているランダムノイズを除去することを特徴とするデータ復号方法。

【請求項１１】　一連の連続したデータ列のプログラムを暗号化して送出するデータ送出装置と、送出されてきたプログラムを復号する復号装置から成る伝送システムにおいて、

上記データ送出装置は、

ランダムノイズを発生するランダムノイズ発生手段と、

上記ランダムノイズ発生手段で発生したランダムノイズを上記プログラムの前後に付加する付加手段と、

上記付加手段にてランダムノイズが付加されたプログラムに対して暗号化処理を行う暗号化手段と、

上記暗号化手段により暗号化されたランダムノイズが付加されたプログラムを送出する送出手段と、

を備え、

上記データ復号装置は、

送出されてきたプログラムを入力する入力手段と、

上記入力手段により入力されたプログラムに対して暗号化を解読する復号処理を行う復号手段と、

上記復号手段で復号されたプログラムの前後に付加されているランダムノイズを除去する除去手段と、

を備えたことを特徴とする伝送システム。

【請求項１２】　上記付加手段で付加するランダムノイズのデータ長は可変長とされていることを特徴とする請求項１１に記載の伝送システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は暗号化されたプログラムデータの伝送を行う伝送システム、及びパケットデータの伝送にかかるデータ送出装置、データ復号装置、データ送出方法、データ復号方法に関するものである。

【０００２】

【従来の技術】

例えば著作権保護が必要なデータ、秘密性の高いデータ、プライバシーにかかる私的データなど、外部に漏洩することが好ましくないデータの伝送に際しては、暗号化処理が行われることが多い。例えば音楽データ、映像データなど、一連の連続したデータ列としてのプログラムの伝送に際しては、著作権保護の必要性などから暗号化が行われて伝送されることが行われている。なお、本明細書でいう「プログラム」とは、一連のデータ列としてデータ群のことであり、例えば一般に１つの楽曲のデータに相当する「トラック」とも呼ばれるものを含む広義のものである。

【０００３】

図１１に或る送信装置１０１から受信装置１０２に対してプログラムデータを暗号化して伝送するモデルを示す。

いま、伝送しようとするデータＤＴが送信装置１０１に入力されたとすると、

送信装置１０１は、まず暗号化部１１１で暗号化処理を施し、暗号化されたデータＤＴｓを生成する。

そしてそのデータＤＴｓは送信部１１２から送信出力される。

送信出力されたデータＤＴｓは例えばＩＥＥＥ１３９４バスなどの伝送路１０３により、受信装置１０２に送られることになる。

受信装置１０２では、伝送路１０３から送信されてきたデータＤＴｓを受信部１２１で受信し、復号部１２２で暗号解読処理を行うことで、元のデータＤＴを得ることができる。

【０００４】

【発明が解決しようとする課題】

このように伝送路１０３においては暗号化されたデータＤＴｓが送信されることで、仮に伝送路１０３においてデータＤＴｓが取り出されたとしても、データＤＴの内容は秘密性が保たれるものとなる。

しかしながら、例えば著作権保護を目的として音楽データ等を図１１のようなシステムで伝送する場合、暗号を解読され、結果として違法なコピーが行われるおそれがある。

【０００５】

例えば伝送しようとするプログラムとしてのデータＤＴがＰＣＭオーディオデータであったとする。

ＰＣＭオーディオデータの場合、無音部分では、データストリーム上でゼロデータが並んでいるものとなっている。又は例えばΔΣ変調された１ビットオーディオデータの場合、無音部分は「９６ｈ」（＝１００１０１１０）などの固定パターンとなっている。

音楽トラックとしてのプログラムデータを考えると、そのプログラムの先頭部分と終端部分は、多くの場合、無音となっている。つまり、例えば２つの曲（プログラム）が、音楽としてメドレー形式でつながっている場合などを除いては、曲の頭（曲が開始される直前）と終わり（曲が終了した直後）はデータとしては無音部分が存在していることが殆どである。

【０００６】

ここで、図１１に破線で示すように、何らかの手段で伝送路１０３から暗号化されたデータＤＴｓが取り出されたとする。

通常は、データＤＴｓを解析しても、元のデータＤＴ自体がわからないため、暗号の解読は困難である。

ところが、データＤＴｓにおいて、プログラムデータＤＴのうちで曲の先頭部分又は終端部分、即ち無音部分に相当する部分を抽出されると、元のデータがゼロデータ等の固定パターンであること、つまり元のデータの内容が明白となっている場合が多いことから、比較的容易に暗号が解読され、データＤＴの内容や暗号化アルゴリズムが知られてしまう危険性がある。

もちろん暗号化アルゴリズムが解読されれば、悪意のユーザーによればその後データＤＴの違法な取り込みが容易に可能となってしまう。つまり著作権侵害となるような行為を実行可能としてしまう。

【０００７】

従って、音楽データ等の著作権保護が必要なデータについて、機器間の伝送、記録媒体への記録のための伝送、或いは公衆回線等を用いた音楽配信システムにおける伝送などの広範囲の分野で、上記の危険性が内包されており、このため違法な暗号解読を防止できるような技術が求められている。

【０００８】

【課題を解決するための手段】

本発明はこのような状況に鑑みて、伝送されるデータについて、容易に暗号解読ができないようにする技術を提供するものである。

【０００９】

このため本発明では、一連の連続したデータ列のプログラムを暗号化して送出するデータ送出装置において、ランダムノイズを発生するランダムノイズ発生手段と、上記ランダムノイズ発生手段で発生したランダムノイズを上記プログラムの前後に付加する付加手段と、上記付加手段にてランダムノイズが付加されたプログラムに対して暗号化処理を行う暗号化手段と、上記暗号化手段により暗号化されたランダムノイズが付加されたプログラムを送出する送出手段とを備えるよ

うにする。

また、上記付加手段で付加するランダムノイズのデータ長は可変長とされているようにする。

【００１０】

また本発明は、一連の連続したデータ列の前後にランダムノイズが付加され、暗号化が施されたプログラムを入力して復号するデータ復号装置において、送出されてきたプログラムを入力する入力手段と、上記入力手段により入力されたプログラムに対して暗号化を解読する復号処理を行う復号手段と、上記復号手段で復号されたプログラムの前後に付加されているランダムノイズを除去する除去手段とを備える。

【００１１】

また、本発明の伝送システムは、上記構成のデータ送出装置と上記構成のデータ復号装置により構成されるものとする。

そしてデータ送出装置とデータ復号装置は、それぞれ異なる機器間における送信装置、受信装置としたり、記録媒体に記録を行う記録装置における記録データの送出装置、記録媒体からデータの再生を行う再生装置における再生データの復号装置などとして実現されるようにする。

【００１２】

本発明のデータ伝送方法は、一連の連続したデータ列のプログラムの前後にランダムノイズを付加し、ランダムノイズが付加されたプログラムに対して暗号化処理を行ない、暗号化されたランダムノイズが付加されたプログラムを送出する。

ここで、プログラムの前後に付加するランダムノイズのデータ長は可変長とする。

本発明のデータ復号方法は、一連の連続したデータ列の前後にランダムノイズが付加され、暗号化が施されたプログラムを入力し、入力されたプログラムに対して暗号化を解読する復号処理を行ない、復号されたプログラムの前後に付加されているランダムノイズを除去する。

【００１３】

即ち本発明では、暗号化を行う前にプログラム（曲データ等）の前後にランダムノイズを付加する。これによって、例えば元のデータにおいて曲の前後に無音部分が存在しても、ランダムノイズが付加されることで曲の先頭及び終端が無音データとはならない状態とされた上で暗号化されることとなるため、暗号化されたプログラムの先頭部分又は終端部分が抽出されて解析されても、暗号アルゴリズムの解読は非常に困難なものとなる。また付加するランダムノイズのデータ長は可変長とすることで無音データ部分が位置的に不明確になり、暗号解読防止効果を高めることができる。

【００１４】

【発明の実施の形態】

以下、本発明の実施の形態を次の順に説明する。

１．送信装置及び受信装置に本発明を採用する例
２．ＩＥＥＥ１３９４の伝送フォーマット
３．ＩＥＥＥ１３９４でのデータ伝送の場合のランダムノイズ付加例
４．記録装置及び再生装置に本発明を採用する例

【００１５】

１．送信装置及び受信装置に本発明を採用する例

本発明のデータ送出装置（データ送出方法）、データ復号装置（データ復号方法）を、送信装置、受信装置に採用する実施の形態を説明する。

図１は、或る２つの機器が例えばＩＥＥＥ１３９４バスによる伝送路３により接続されている場合に、送信装置１を有する機器から受信装置２を有する機器にプログラムデータＤＴを伝送するモデルにおいて本発明の実施の形態を示したものである。

詳しくは後述するが、データＤＴは、例えば１ビットデジタルオーディオデー

タを、所定の伝送プロトコルに合致するフォーマットに基づいてパケット化（ブロック化）したものであるとする。

【００１６】

１ビットデジタルオーディオデータとは、通常のＣＤ（Compact Disc）におけるオーディオデータよりも高品位なデータとして開発されたものであり、サンプリング周波数を例えばＣＤ方式における４４．１ＫＨｚの１６倍という非常に高いサンプリング周波数である２．８４２ＭＨｚとしてΔΣ変調された１ビットデータのことであり、周波数帯域はＤＣ成分～１００ＫＨｚの広範囲とされ、ダイナミックレンジはオーディオ帯域全体で１２０（ｄＢ）を実現できるデータ形式である。

なお、本例ではこのような１ビットデジタルオーディオデータをパケット化して伝送する場合を例に挙げるが、もちろん伝送されるデータ自体の形式、種別はどのようなものでもよい。

【００１７】

図示するように送信装置１は、ランダムノイズ付加部１１，暗号化部１２、送信部１３、ランダムノイズ発生部１４が設けられる。

ランダムノイズ発生部１４は例えば乱数発生回路によりランダムノイズ（乱数データ）を発生させ、ランダムノイズ付加部１１に供給する。

ランダムノイズ付加部１１は、送信しようとするデータＤＴに対して、プログラム（楽曲等）の先頭部分及び終端部分に、上記ランダムノイズ発生部１４で発生されたランダムノイズを付加する動作を行う。

暗号化部１２は、ランダムノイズ付加部１１の出力に対して所定の暗号アルゴリズムでの暗号化処理を施す。

送信部１３は暗号化部１２の出力をＩＥＥＥ１３９４バスによる伝送路３に送出する動作を行う。

【００１８】

受信装置２は、受信部２１，復号部２２、ランダムノイズ除去部２３を備える。

受信部２１は、伝送路３から供給されるデータを受信して取り込む動作を行う

。

復号部２２は、上記暗号化部１２での暗号化アルゴリズムに対応して暗号解読処理を行う部位である。

ランダムノイズ除去部２３は、上記ランダムノイズ付加部１１で付加されたランダムノイズ部分を除去する部位である。

【００１９】

このような送信装置１、受信装置２においてデータＤＴの伝送は次のように行われる。図２を参照しながら説明する。

図２（ａ）はプログラム（トラック）として１曲が構成されている楽曲データを示している。これがデータＤＴとして伝送しようとするオーディオデータソースである。そして音楽データの場合、トラックデータの先頭部分と終端部分は図２（ｂ）のように無音となっている場合が多い。

【００２０】

例えば楽曲等のプログラムデータとして、図２（ａ）（ｂ）に示すデータＤＴが送信装置１に入力されたとすると、送信装置１は、まずランダムノイズ付加部１１で、データＤＴにおけるプログラムの先頭及び終端に相当する部分に、任意のデータ長としてのランダムノイズを挿入する。例えば図２（ｃ）のように、トラックの先頭部分に時間長Ｔａｄ１のデータサイズのランダムノイズを付加し、またトラックの終端部分に時間長Ｔａｄ２のデータサイズのランダムノイズを付加する。具体例は後述するが、例えばランダムノイズが充填されたブロックをパケットデータに付加する。

なお、時間長Ｔａｄ１、Ｔａｄ２、即ち付加するランダムノイズのデータ長は、一定としてもよいが、可変長、即ち付加処理を行うたびに毎回ランダムな長さとしたり、送信装置１としての機器毎に任意に設定する長さとしてもよい。付加するランダムノイズのデータ長のランダム性が高いほど、実際の無音データ部分がより不明確となるため、不正な暗号解読をより困難にできる。

【００２１】

ランダムノイズ付加部１１でランダムノイズが付加されたデータＤＴａｄは、続いて暗号化部１２に供給され、暗号化処理が施される。即ち図２（ｄ）のよう

に、ランダムノイズ部分、無音を含めた音楽データ部分が、それぞれ暗号化された状態となる。

暗号化されたデータＤＴｓは、送信部１３に供給され、送信部１３から伝送路３に対して送出されることになる。

【００２２】

このように送信されたデータＤＴｓを受信する受信装置２では、まず伝送路３から供給されてきたデータＤＴｓを受信部２１で受信し、復号部２２に供給する。復号部ではデータＤＴｓに対する暗号解読処理を行うことで、暗号化前のデータ、即ち図２（ｃ）のようにランダムノイズが付加されている状態のデータＤＴａｄが出力される。

このデータＤＴａｄはランダムノイズ除去部２３に供給され、ランダムノイズ部分が除去されることで、当初の送信データ、即ち図２（ｂ）のようなデータＤＴが得られることとなる。

【００２３】

ここで図１に破線で示すように、何らかの手段で伝送路３から暗号化されたデータＤＴｓが取り出された場合を考える。

上述したようにデータＤＴｓにおいて元の内容が明白な無音部分が抽出されると暗号化アルゴリズムが解読されるおそれがある。そして無音部分としては通常、トラックの先頭部分及び終端部分である。従って、データＤＴｓにおいてトラックの先頭部分又は終端部分に相当する部分が不正な暗号解読に用いられると、暗号解読に有利となってしまう。

【００２４】

しかしながら本例の場合、データＤＴｓは、トラックの先頭及び終端にランダムノイズが付加された上で暗号化されたものである。つまりトラックの先頭及び終端はゼロデータ等の固定パターンが連続する部分ではないものとされた状態で暗号化されている。従ってデータＤＴｓにおいてトラックの先頭又は終端に相当する部分が抽出されたとしても、元のデータはランダムノイズであることから、元のデータは予測できず、暗号解読は困難となる。

特にデータＤＴｓの解析処理において、データＤＴｓ上では暗号化アルゴリズ

ムによるデータ要素とランダムノイズによるデータ要素を区別することはできず、暗号化アルゴリズムを解析することはほぼ不可能である。

さらに、付加するランダムノイズのデータ長が可変長であることで、不正な解読を行おうとする者が、実際のゼロデータもしくは固定パターンが連続する部分を予測することは著しく困難となり、この点で暗号解読に対する安全性を高めることができる。

【００２５】

以上のことから、本例によれば伝送路３で伝送されるデータについて暗号解読は非常に困難なものとなり、従って、著作権保護を要するデータの伝送などに非常に好適なものとなる。

また送信装置１側では従前の構成にランダムノイズ付加部１１及びランダムノイズ発生部１４を設けるだけでよく、受信装置２側では、ランダムノイズ除去部２３を設けて、暗号化を解読したうえでランダムノイズが挿入されたデータ部分を除去するのみでデータを復号できる。従って送信装置１，受信装置２としての構成がさほど複雑化することもなく、各種の機器への導入は容易なものとなる。

【００２６】

２．ＩＥＥＥ１３９４の伝送フォーマット

ここでＩＥＥＥ１３９４による伝送フォーマットについて説明する。

ＩＥＥＥ１３９４方式でのデータ伝送では、例えば図３（ａ）に示すように、所定の通信サイクル（例えば１２５μｓｅｃ）毎に時分割多重によって行われる。そして、この信号の伝送は、サイクルマスタと呼ばれる機器（ＩＥＥＥ１３９４バス上の任意の１台の機器）が通信サイクルの開始時であることを示すサイクルスタートパケットＣＳＰをバス上へ送出することにより開始される。なお、サイクルマスタは、バスを構成するケーブルに各機器を接続したとき等に、ＩＥＥＥ１３９４で規定する手順により自動的に決定される。

【００２７】

１通信サイクル中における通信の形態は、ビデオデータやオーディオデータなどのリアルタイム性を必要とするデータを伝送するアイソクロナス伝送（Ｉｓｏ）と、制御コマンドや補助的なデータなどを確実に伝送するアシンクロナス伝送（Ａｓｙ）の２種類の伝送が行われる。

各通信サイクル中では、アイソクロナス伝送用のアイソクロナスパケットＩｓｏが、アシンクロナス伝送用のアシンクロナスパケットＡｓｙより先に伝送される。

アイソクロナスパケットＩｓｏの通信が終了した後、次のサイクルスタートパケットＣＳＰまでの期間が、アシンクロナスパケットＡｓｙの伝送に使用される。従って、アシンクロナスパケットＡｓｙが伝送できる期間は、そのときのアイソクロナスパケットＩｓｏの伝送チャンネル数により変化する。また、アイソクロナスパケットＩｓｏは、１通信サイクル毎に予約した帯域（チャンネル数）が確保される伝送方式であるが、受信側からの確認は行わない。

アシンクロナスパケットＡｓｙで伝送する場合には、受信側からアクノリッジメント（Ａｃｋ）のデータを返送させて、伝送状態を確認しながら確実に伝送させる。

【００２８】

図３（ｂ）に、ＣＩＰ(Common Isochronos Packet)の構造を示す。つまり、図３（ａ）に示したアイソクロナスパケットＩｓｏのデータ構造である。

例えば、上述した１ビットデジタルオーディオデータは、ＩＥＥＥ１３９４通信においては、アイソクロナス通信によりデータの送受信が行われる。つまり、リアルタイム性が維持されるだけのデータ量をこのアイソクロナスパケットに格納して、１アイソクロナスサイクル毎に順次送信するものである。

【００２９】

アイソクロナスパケットは、図３（ｂ）のように、１３９４パケットヘッダ、ヘッダＣＲＣ、ＣＩＰヘッダ、データ部、データＣＲＣから成る。

このＣＩＰ構造として、例えば２チャンネルの１ビットデジタルオーディオデータの伝送に用いる場合における具体例を図４に示している。

【００３０】

図４では、横方向に３２ビット（４バイト）を示しているが、その１行分のデータ、つまり３２ビットが１カドレット（ｑｕａｄｌｅｔ）と呼ばれる。

ＣＩＰの先頭３２ビット（１カドレット）は、１３９４パケットヘッダとされている。

１３９４パケットヘッダにおいては、１６ビットのデータレングス（ｄａｔａ＿Ｌｅｎｇｔｈ）、２ビットのタグ（ｔａｇ）、６ビットのチャンネル（ｃｈａｎｎｅｌ）、４ビットのタイムコード（ｔ　ｃｏｄｅ）、４ビットのシンク（ｓｙ）が配される。

そして、１３９４パケットヘッダに続く１カドレットの領域はヘッダＣＲＣが格納される。

【００３１】

ヘッダＣＲＣに続く２カドレットの領域がＣＩＰヘッダとなる。

ＣＩＰヘッダの上位カドレットの先頭２バイトには、それぞれ‘０’‘０’が格納され、続く６ビットの領域はＳＩＤ（送信ノード番号）を示す。ＳＩＤに続く８ビットの領域はＤＢＳ（データブロックサイズ）であり、データブロックのサイズ（パケット化の単位データ量）が示される。続いては、ＦＮ（２ビット）、ＱＰＣ（３ビット）の領域が設定されており、ＦＮにはパケット化する際に分割した数が示され、ＱＰＣには分割するために追加したカドレット数が示される。

ＳＰ（１ビット）にはソースパケットのヘッダのフラグが示され、ＤＢＣにはパケットの欠落を検出するカウンタの値が格納される。

なお、図中「ｒｓｖ」はリザーブ、つまり未定義の領域を示している。

【００３２】

ＣＩＰヘッダの下位カドレットの先頭２バイトにはそれぞれ‘１’‘０’が格納される。そして、これに続いてＦＭＴ（６ビット）、ＦＤＦ（８ビット）、ＳＹＴ（１６ビット）の領域が設けられる。

ＦＭＴには信号フォーマット（伝送フォーマット）が示され、ここに示される値によって、当該ＣＩＰに格納されるデータ種類（データフォーマット）が識別

可能となる。具体的には、ＭＰＥＧストリームデータ、Ａｕｄｉｏストリームデータ、デジタルビデオカメラ（ＤＶ）ストリームデータ等の識別が可能になる。

ＦＤＦは、フォーマット依存フィールドであり、上記ＦＭＴにより分類されたデータフォーマットについて更に細分化した分類を示す領域とされる。オーディオに関するデータであれば、例えばリニアオーディオデータであるのか、ＭＩＤＩデータであるのかといった識別が可能になる。

例えば１ビットデジタルオーディオデータであれば、先ずＦＭＴによりＡｕｄｉｏストリームデータの範疇にあるデータであることが示され、ＦＤＦに規定に従った特定の値が格納されることで、そのＡｕｄｉｏストリームデータは１ビットデジタルオーディオデータであることが示される。

ＳＹＴは、フレーム同期用のタイムスタンプが示される。

【００３３】

このようなＣＩＰヘッダに続けては、ＦＭＴ，ＦＤＦによって示されるデータが、データ部としてのｎ個のデータブロック（ブロック＃０～＃ｎ）のシーケンスによって格納される。ＦＭＴ，ＦＤＦにより１ビットデジタルオーディオデータであることが示される場合には、このデータブロックとしての領域に１ビットデジタルオーディオデータが格納される。

そして、データブロックに続いて最後にデータＣＲＣが配置される。

【００３４】

この図４では、データ部に２チャンネルの１ビットデジタルオーディオデータが配されている例を示している。これは、ＩＥＥＥ１３９４バスによるデータ伝送について適用できるＡＭ８２４と呼ばれる伝送プロトコルに基づいた例であり、その場合において１ビットデジタルオーディオデータとして２チャンネルのオーディオデータを伝送する場合のパケット構造例である。

【００３５】

上述のように３２ビット（４バイト）を１カドレット（Quadlet）と呼ぶとすると、２チャンネルデータの場合、４カドレット（ｑ１～ｑ４）で１つのブロックが形成され、このブロックが連続するものとなる。

【００３６】

各カドレットにおける先頭のバイト（バイト０）は、ラベルとされている。ラベルとは、そのカドレットに配されるデータの識別情報となる。

ラベルとしての値及び意味を図５に示す。

図示するようにラベル値に対して各種の意味が定義されており、例えばラベル値４０ｈ～４Ｆｈは、ＤＶＤ（Digital Versatile Disc）システムで採用されているマルチビットリニアオーディオデータに対応するものとされる。なお、「ｈ」を付した数値は１６進表記のものである。

またラベル値５０ｈ～５７ｈは、１ビットデジタルオーディオデータに対応する値、ラベル値５８ｈ～５Ｆｈは、エンコードされた１ビットデジタルオーディオデータに対応する値、ラベル値８０ｈ～８３ｈはＭＩＤＩデータに対応する値とされる。

さらにＣ０ｈ～ＥＦｈはアンシラリデータ（Ancillary Data；補助データ）を意味するなど、ラベル値は識別情報として機能するために各種定義されている。

【００３７】

各ラベル値についての詳細な定義の説明は本発明と直接関係がないため説明を省略するが、図４に示した値についてのみ述べると次のようになる。

【００３８】

図４においてブロック＃０の第１カドレットｑ１をみると、ラベル値は「Ｄ１ｈ」とされている。従って第１カドレットｑ１はアンシラリデータが記述されるものと提示されていることになり、さらにこの場合バイト１はサブラベルとされて「００ｈ」とされている。

このときバイト２，バイト３が実際の補助データ内容となるが、ここではバリディティフラグ（Validity Flag）Ｖ、コピーコントロール情報（Track Attribute）、チャネル数（Ch Bit Num）、スピーカ配置情報（Loudspeaker Config）が記述される。

【００３９】

第２カドレットｑ２ではラベル値は「５０ｈ」とされる。ラベル値５０ｈ～５７ｈは、１ビットデジタルオーディオデータに対応する値であるが、「５０ｈ」

は、マルチチャンネルのデータを配したブロックの最初のデータであることを示す。

また第３カドレットｑ３ではラベル値は「５１ｈ」とされる。「５１ｈ」は、マルチチャンネルのデータを配したブロックの２番目以降のデータであることを示す。

従って、第２、第３カドレット（ｑ２、ｑ３）では、チャンネル１、チャンネル２の２チャンネルの１ビットデジタルオーディオデータが配されていることが示されるものとなる。各チャンネルのデータはバイト１～バイト３の３バイトで記述される。

【００４０】

第４カドレットｑ４では、ラベル値は「ＣＦｈ」とされている。これはアンシラリデータの範疇であるが、「ＣＦｈ」は特に無効データ（NO DATA）を示す値として定義されている。またバイト１はサブラベルとして無効データの内容を示す値とされており、この例では「ＣＦｈ」とされている。

そしてこのときバイト２，バイト３が無効データにより充填される。

【００４１】

ブロック＃１の第１カドレットｑ１では、ラベル値は「Ｄ１ｈ」とされている。従って第１カドレットｑ１はアンシラリデータが記述されるものと提示されていることになり、さらにこの場合バイト１はサブラベルとされて「０１ｈ」とされている。

このときはバイト２，バイト３の補助データ内容は、サプリメンタリデータとされる。

第２～第４カドレットはブロック＃０と同様である。

【００４２】

このように各ブロックが構成されて、アイソクロナスパケットＩｓｏにおけるデータ部が形成される。

【００４３】

３．ＩＥＥＥ１３９４でのデータ伝送の場合のランダムノイズ付加例

以上のようなＩＥＥＥ１３９４による伝送フォーマットを用いて、図１で説明したようにデータを伝送する場合の具体例を以下、説明していく。即ちＩＥＥＥ１３９４の伝送路３でオーディオパケットデータを伝送する場合のランダムノイズ付加方式の例である。

【００４４】

上記図４で示したデータ部を構成するブロック＃０、＃１・・・に配されるオーディオデータは、元々の１ビットデジタルオーディオデータとしてのプログラムから見ると図６に示す関係となる。

図６（ａ）は１つの楽曲としてのデータ群となるトラック（プログラム）をトラック＃Ｎとして示しているが、このトラック＃Ｎは図６（ｂ）のように複数のフレームから構成される。

公知のように１つのフレームは７５Ｈｚ周期、即ち１３．３ｍｓｅｃ分のオーディオデータに相当する単位である。

そして図６（ｃ）のように１フレームは１５６８ブロック（ブロック＃０～＃１５６７）で構成される。

【００４５】

図７は送信しようとするデータＤＴとしてのデータパケット構造例を示している。これは、ＩＥＥＥ１３９４バスによるデータ伝送について適用できるＡＭ８２４の伝送プロトコルに基づき、１ビットデジタルオーディオデータとして６チャンネルのオーディオデータを伝送する場合のパケット構造例を示しているものである。

なお、図７にフレームとして示すブロック＃０～＃１５６７の部分は、図３，図４で説明したアイソクロナスパケットＩｓｏ内のデータ部に相当する部分である。

【００４６】

６チャンネルデータの場合、８カドレット（ｑ１～ｑ８）で１つのブロックが形成され、このブロックが連続するものとなる。

１５６８ブロックの範囲が１フレームとなる。

そして１ビットデジタルオーディオデータとしての伝送データストリームは、このようなフレームが連続されて形成される。

【００４７】

この場合、ブロック＃０の第１カドレットｑ１をみると、ラベル値は「Ｄ１ｈ」とされている。従って第１カドレットｑ１はアンシラリデータが記述されるものと提示されていることになり、さらにこの場合バイト１はサブラベルとされて「００ｈ」とされている。図３で説明したように、バイト２，バイト３の補助データ内容としては、コピーコントロール情報、チャネル数、スピーカ配置情報等が記述される。

【００４８】

第２カドレットｑ２ではラベル値は「５０ｈ」とされる。ラベル値５０ｈ～５７ｈは、１ビットデジタルオーディオデータに対応する値であるが、「５０ｈ」は、マルチチャンネルのデータを配したブロックの最初のデータであることを示す。

また第３～第７カドレット（ｑ３～ｑ７）ではラベル値は「５１ｈ」とされる。「５１ｈ」は、マルチチャンネルのデータを配したブロックの２番目以降のデータであることを示す。

従って、第２～第７カドレット（ｑ１～ｑ７）では、チャンネル１～チャンネル６の６チャンネルの１ビットデジタルオーディオデータが配されていることが示されるものとなる。各チャンネルのデータはバイト１～バイト３の３バイトで記述される。

【００４９】

第８カドレットｑ８では、ラベル値は「ＣＦｈ」とされている。これはアンシラリデータの範疇であるが、「ＣＦｈ」は特に無効データ（NO DATA）を示す値として定義されている。

またこの場合は、バイト１は無効データの内容を示す値とされており、この例のような「５０ｈ」は１ビットデジタルオーディオデータとしての無効データを示すものとなる。

そしてこのときバイト２，バイト３が無効データにより充填される。

【００５０】

ブロック＃１の第１カドレットｑ１では、ラベル値は「Ｄ１ｈ」とされている。従って第１カドレットｑ１はアンシラリデータが記述されるものと提示されていることになり、さらにこの場合バイト１はサブラベルとされて「０１ｈ」とされている。

このときはバイト２，バイト３の補助データ内容は、サプリメンタリデータとされる。

第２～第８カドレットはブロック＃０と同様である。

【００５１】

ブロック＃１５６７の第１カドレットｑ１では、ラベル値は「ＣＦｈ」とされている。つまりバイト２，バイト３は無効データである。ただし、バイト１は「Ｄ１ｈ」とされていることで、アンシラリデータとしての無効データであることが示されている。

第２～第８カドレットはブロック＃０と同様である。

【００５２】

例えばこのようなパケットデータストリームを伝送する場合を例に挙げると、上述した送信装置１のランダムノイズ付加部１１では、図７のような連続するブロックによって構成されるトラックの先頭及び終端に、図８のようなブロックを任意の長さ（ランダムなデータ量）だけ付加するものとなる。

【００５３】

図８のブロックは、図７と同じく８カドレット（ｑ１～ｑ８）で構成されるが、全てのカドレットは、ラベルが「ＣＦｈ」とされている。即ち無効データであることが示される。またサブラベルとして、「Ｄ１ｈ」「５０ｈ」「ＣＦｈ」等が配される。

そして全カドレットｑ１～ｑ８のバイト２，３（斜線部）には、ランダムノイズが充填される。

【００５４】

このようなランダムノイズが充填されたブロックをトラックの先頭及び終端に

任意のブロック数だけ付加することで、図２（ｃ）に示したような状態とする。そして上述した図２（ｄ）のように暗号化が施されて送出される。

これによって、伝送される暗号化データＤＴｓから仮にトラックの先頭又は終端に相当する部分が抽出されたとしても、その部分は暗号化前のデータがランダムノイズであるため、上述の通り、暗号解読を防止できるものとなる。

【００５５】

また、このように無効データであることを示すラベル「ＣＦｈ」を設定したブロック内の各カドレットにランダムノイズを配することは、受信装置２側での処理が非常に簡単となることを意味する。

即ち受信装置１０２の復号部２２で暗号解読処理が施されると、図７，図８の状態のパケットデータストリームがランダムノイズ除去部２３に供給されることになるが、ランダムノイズ除去部２３では、ラベル値＝「ＣＦｈ」のカドレットを捨てればよいのみとなる。

ラベル値＝「ＣＦｈ」のカドレットは無効データとして本来捨てられるものであるため、その意味でいえば、ランダムノイズ除去部２３は何ら特別な処理を必要とせずに、図７における無効データとともに、図８におけるランダムノイズを除去できるものともなる。

【００５６】

４．記録装置及び再生装置に本発明を採用する例

続いて、本発明のデータ送出装置（データ送出方法）、データ復号装置（データ復号方法）を、記録装置、再生装置に採用する実施の形態を説明する。

記録装置は記録媒体に対するデータ送出装置となり、また再生装置は記録媒体から読み出されたデータのデータ復号装置となる。

【００５７】

図９は所定の記録媒体（メディア）６に対してデータＤＴを記録できる記録装置である。

図示するように記録装置４は、入力されてくるデータＤＴに対する記録処理系として、暗号化部４０，エンコード及び記録ドライブ部４４、記録ヘッド（又はインターフェース）４５が設けられる。

暗号化部４０は、ランダムノイズ付加部４１，暗号化部４２、送出部４３、ランダムノイズ発生部４６を有する。

【００５８】

このような記録装置４では、入力されたデータＤＴについて、ランダムノイズ付加部４１は、ランダムノイズ発生部４６から発生させたランダムノイズを、データＤＴにおけるトラック（プログラム）の先頭及び終端部分に付加する。この場合も付加するランダムノイズのデータ長は可変長とすることで、暗号解読の困難性を高めることができる。

ランダムノイズ付加部４１でランダムノイズが付加されたデータＤＴａｄは、続いて暗号化部４２に供給され、暗号化処理が施される。

暗号化されたデータＤＴｓは、送出部４３に供給され、送出部４３からエンコード及び記録ドライブ部４４に送出される。

【００５９】

エンコード及び記録ドライブ部４４は、供給されたデータＤＴｓに対して、記録を行うメディア６の記録フォーマット、変調方式に応じてエラー訂正符号の付加や各種エンコード処理を行い、記録ドライブ信号を生成する。

その記録ドライブ信号は記録ヘッド４５に供給されて記録ヘッド４５によりメディア６へのデータ書込が行われる。

例えばメディア６が光ディスク、光磁気ディスク、磁気ディスク、磁気テープなどであれば、記録ドライブ信号に応じて光学ヘッド又は磁気ヘッドが駆動されて記録が実行される。

また、メディア６がフラッシュメモリなどによるメモリカードのような形態であれば、インターフェース４５によりメディア６に対して書込アクセスが行われることになる。

【００６０】

図１０は所定の記録媒体（メディア）６からデータＤＴを再生できる再生装置

である。

図示するように再生装置５は、メディア６からデータの読み出しを行う再生ヘッド（又はインターフェース）５４、デコード部５５、復号部５０が設けられる。

復号部５０は、取込部５１，復号部５２、ランダムノイズ除去部５３を備える。

【００６１】

この再生装置５では、例えばメディア６としての光ディスク、光磁気ディスク、磁気ディスク、磁気テープなどから光学ヘッド又は磁気ヘッドとしての再生ヘッド５４によって読み出されたデータ、或いはメディア６としてのメモリカードからインターフェース５４を介した読出アクセスにより読み出されたデータは、デコード部５５で、メディア６の記録フォーマットに応じたデコード処理やエラー訂正処理が行われる。そしてそのデコードされたデータは、即ち記録装置４で暗号化されたデータＤＴｓであり、データＤＴｓは取込部５１により復号部５０内に取り込まれ、復号部５２で暗号解読処理される。

復号部５２で、上記暗号化部４２での暗号化アルゴリズムに対応した暗号解読処理を行うことで、ランダムノイズが付加された状態のデータＤＴａｄとされる。そして、そのデータＤＴａｄがランダムノイズ除去部５３に供給されて、上記ランダムノイズ付加部４１で付加されたランダムノイズ部分が除去されることで、元のデータＤＴが再生されるものとなる。

【００６２】

記録装置４，再生装置５が以上のように構成されることで、メディア６に記録されるデータは、トラックの先頭及び終端にランダムノイズが付加された上で暗号化されたデータＤＴｓがエンコードされたものである。つまりトラックの先頭及び終端はゼロデータ又は「９６ｈ」等の固定データが連続する状態ではないようにされた上で暗号化されたデータが、エンコードされている。

従ってメディア６に記録されたデータをデコードしても、トラックの先頭又は終端は無音部分ではなくなる。このため、その部分が抽出され、データＤＴｓが解析されたとしても、データＤＴｓ上では暗号化アルゴリズムによるデータ要素

とランダムノイズによるデータ要素を区別することはできず、暗号化アルゴリズムを解析することはほぼ不可能である。

【００６３】

つまりこのような記録装置、再生装置によれば、メディア６に記録されるデータについて暗号解読は非常に困難なものとなり、従って、著作権保護を要するデータの記録などに非常に好適なものとなる。また、上述した送信装置１，受信装置２の場合と同様に、記録装置４、再生装置５として構成がさほど複雑化することもなく、導入は容易である。

【００６４】

なお、図９，図１０として記録装置４、再生装置５を分けて示したが、これらの回路構成を１つの機器に設けて、記録再生装置とすることはもちろん可能である。

また、記録装置４（又は記録再生装置）としては、必ずしも暗号化部４０を設けなくてもよい。例えば伝送路３を介して或る送信装置から伝送されてきたデータを記録する記録装置を考えると、その送信装置側が図１に示した構成を備えていれば、記録装置に伝送されてくるデータは、既にランダムノイズが付加された上で暗号化されたデータＤＴｓとなっている。従ってその場合、記録装置は暗号化部４０は不要となる。そして再生装置は、図１０に示した復号部５０を備えることで、伝送され記録されたデータの再生を行うことができるようになる。

例えば音楽等の配信システムなどを想定すると、このような形態が好適なものとなる。

【００６５】

以上、実施の形態を説明してきたが、本発明はさらに多様な構成例が考えられ、また送信装置、受信装置、記録装置、再生装置などの形態で多種多様な機器に導入できるものである。

また、上記例では送信装置１と受信装置２は有線としてのＩＥＥＥ１３９４方式の伝送路３による伝送システムとしたが、他の伝送規格によるものでもよく、また衛星通信、無線電話通信、赤外線伝送などの無線伝送システムに本発明を適用できることはもちろんである。

また、伝送するデータは図７、図８に示したようなブロックデータに限定されるものではなく、あらゆるデータの伝送に本発明を適用できる。

【００６６】

【発明の効果】

以上の説明からわかるように、本発明によれば、伝送するプログラムデータについて、その前後にランダムノイズを付加したうえで暗号化を行なって伝送するようにしている。このため、例えば元の曲データ等においてその先頭又は終端が無音データとしてゼロデータ列などの内容が明確な部分が存在しても、その状態が解消された上で、つまり先頭及び終端がランダムデータとされた上で、暗号化されることとなるため、伝送過程などで暗号化データが抽出されたとしても、暗号アルゴリズムの解読は非常に困難なものとなるという効果があり、従って著作権保護などに好適なものとなる。

また、このようにランダムノイズが付加された上で暗号化されたデータを復号する場合は、暗号化を解読したうえでランダムノイズが挿入されたデータ部分を除去するのみでデータを復号できるため、復号のために複雑な処理は必要なく、簡易な構成で復号装置を実現でる。

換言すれば本発明では、データ送出装置、データ復号装置としては装置構成の複雑化を招かずに、暗号解読が非常に困難なデータ伝送を実現できるものとなる。

【００６７】

また本発明では、データ送出装置側で付加するランダムノイズのデータ長は可変長とすることで、実際の無音データ部分が予測困難となる。これによって暗号解読防止機能を一層高めることができる。

【００６８】

またデータ送出装置とデータ復号装置は、それぞれ異なる機器間における送信装置、受信装置とすることで、機器間のデータ伝送において上記効果を実現できる。

さらにデータ送出装置とデータ復号装置は、それぞれ記録媒体に記録を行う記録装置における記録データの送出装置、記録媒体からデータの再生を行う再生装

置における再生データの復号装置とすることで、記録媒体に記録されているデータ、又は記録再生の過程のデータにおいて上記効果を実現できる。

【図面の簡単な説明】

【図１】

本発明の実施の形態の送信装置及び受信装置のブロック図である。

【図２】

実施の形態のランダムノイズ付加の説明図である。

【図３】

ＩＥＥＥ１３９４による伝送フォーマットの説明図である。

【図４】

ＩＥＥＥ１３９４のアイソクロナスパケットの説明図である。

【図５】

実施の形態のパケットデータのラベルの説明図である。

【図６】

実施の形態のトラック構造の説明図である。

【図７】

実施の形態のランダムノイズ付加例の説明図である。

【図８】

実施の形態のランダムノイズ付加例の説明図である。

【図９】

実施の形態の記録装置のブロック図である。

【図１０】

実施の形態の再生装置のブロック図である。

【図１１】

従来の伝送システムの説明図である。

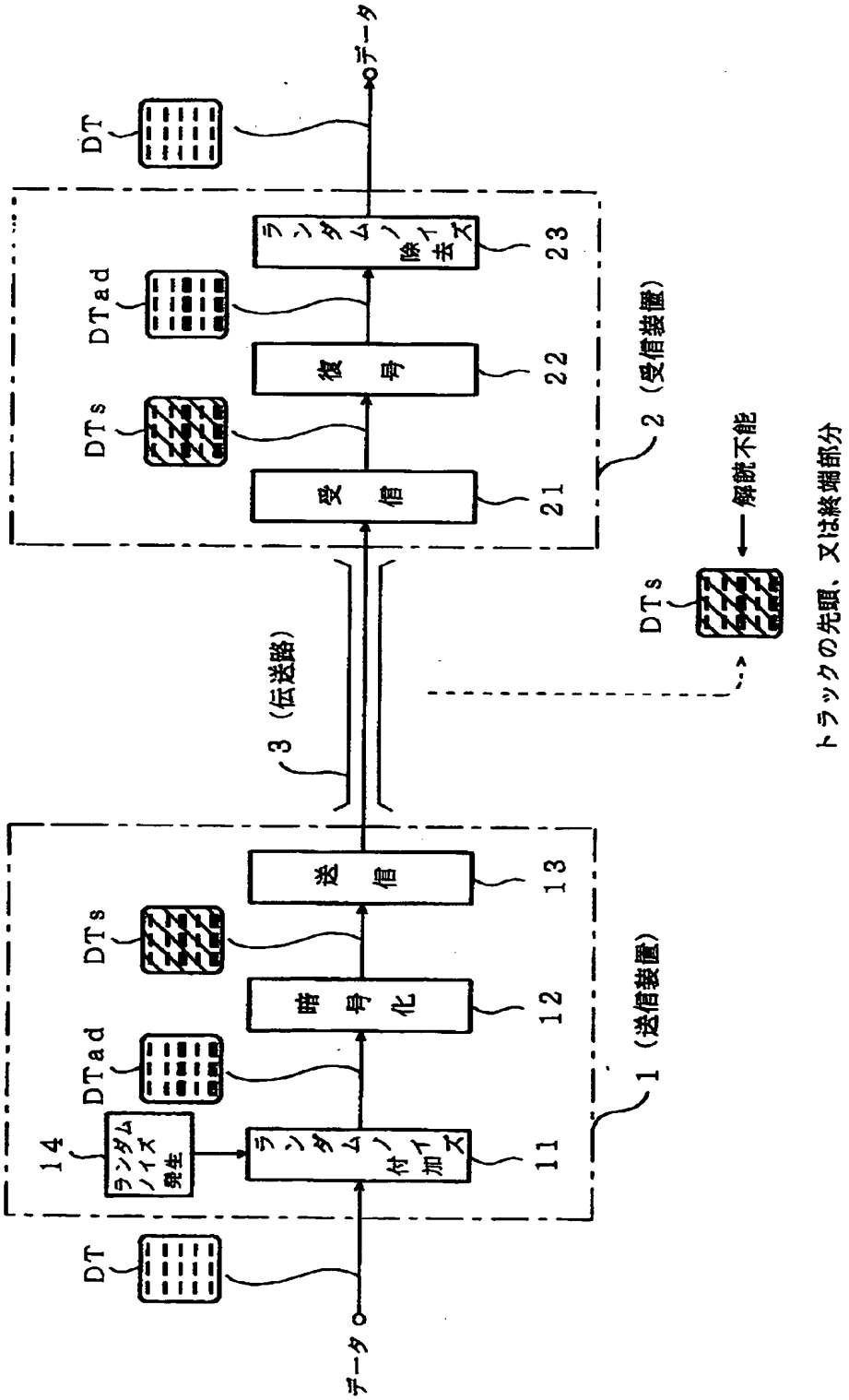
【符号の説明】

１　送信装置、２　受信装置、３　伝送路、４　記録装置、５　再生装置、６　メディア、１１，４１　ランダムノイズ付加部、１２，４２　暗号化部、１３　送信部、１４，４６　ランダムノイズ発生部、２１　受信部、２２，５２　復

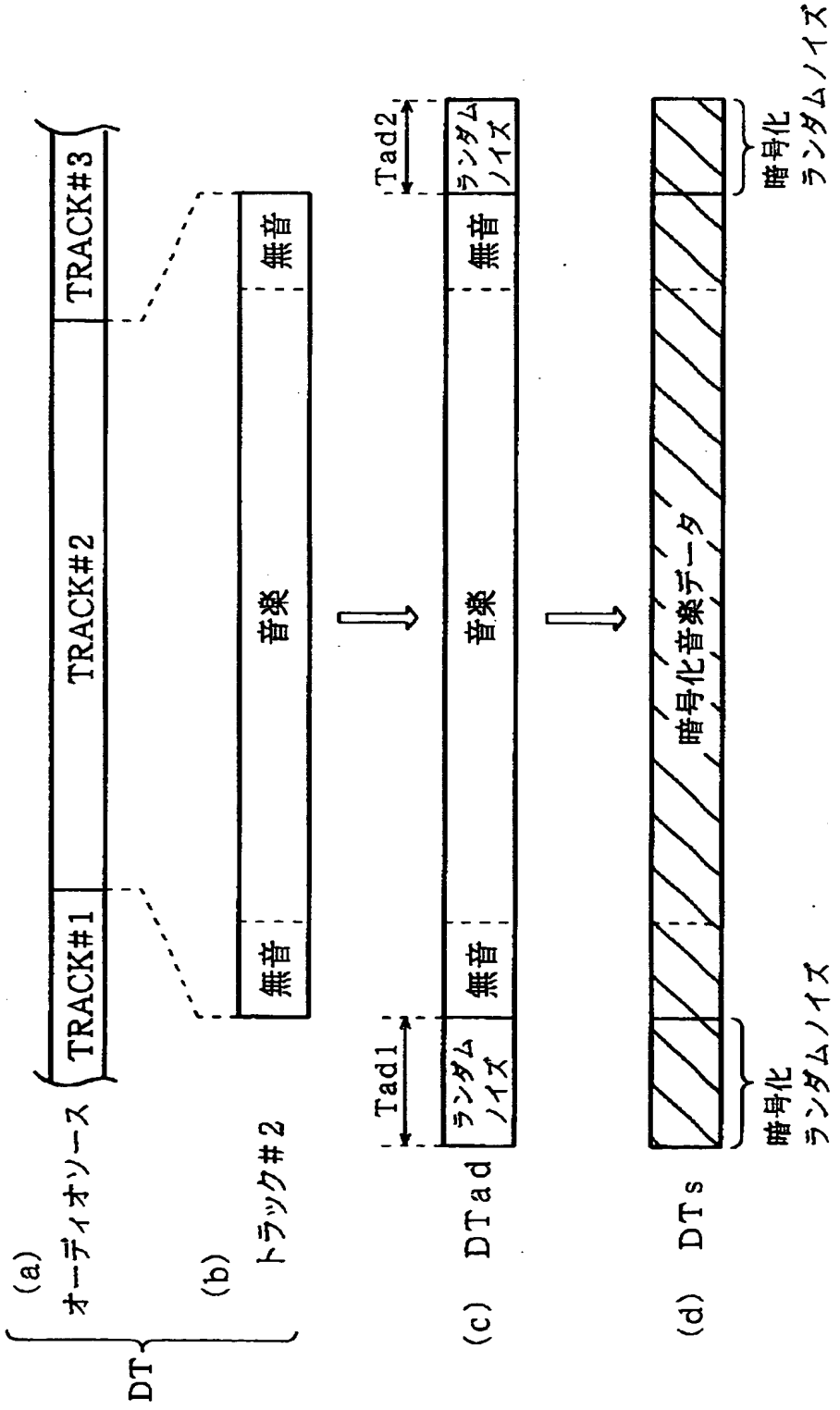
号部、２３，５３　ランダムノイズ除去部、４３　送出部、５１　取込部

【書類名】　　図面

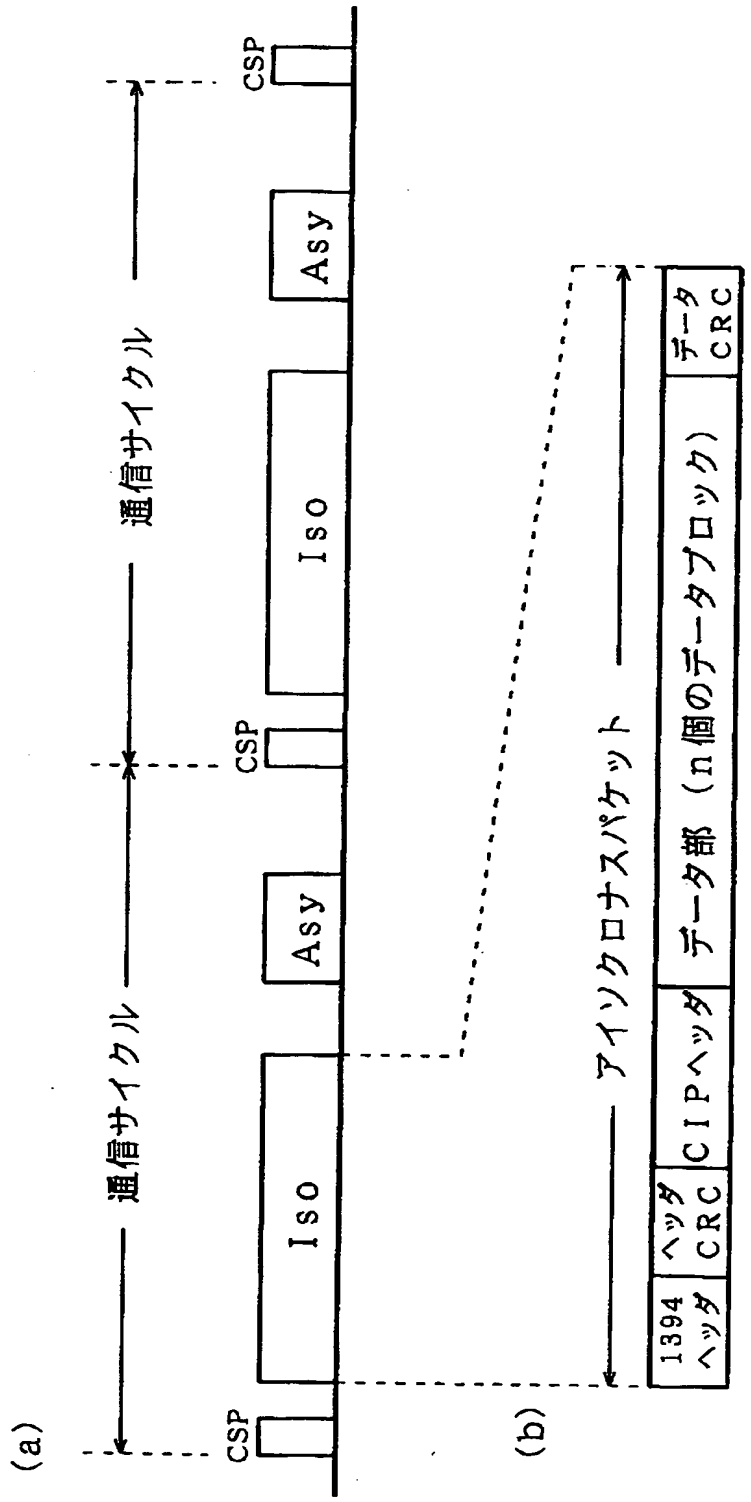
【図１】


データ
DT
ランダムノイズ除去
23
DTad
復号
22
DTs
受信
21
2（受信装置）
解読不能
DTs
トラックの先頭、又は終端部分
3（伝送路）
送信
13
DTs
暗号化
12
DTad
14
ランダムノイズ発生
ランダムノイズ付加
11
1（送信装置）
DT
データ

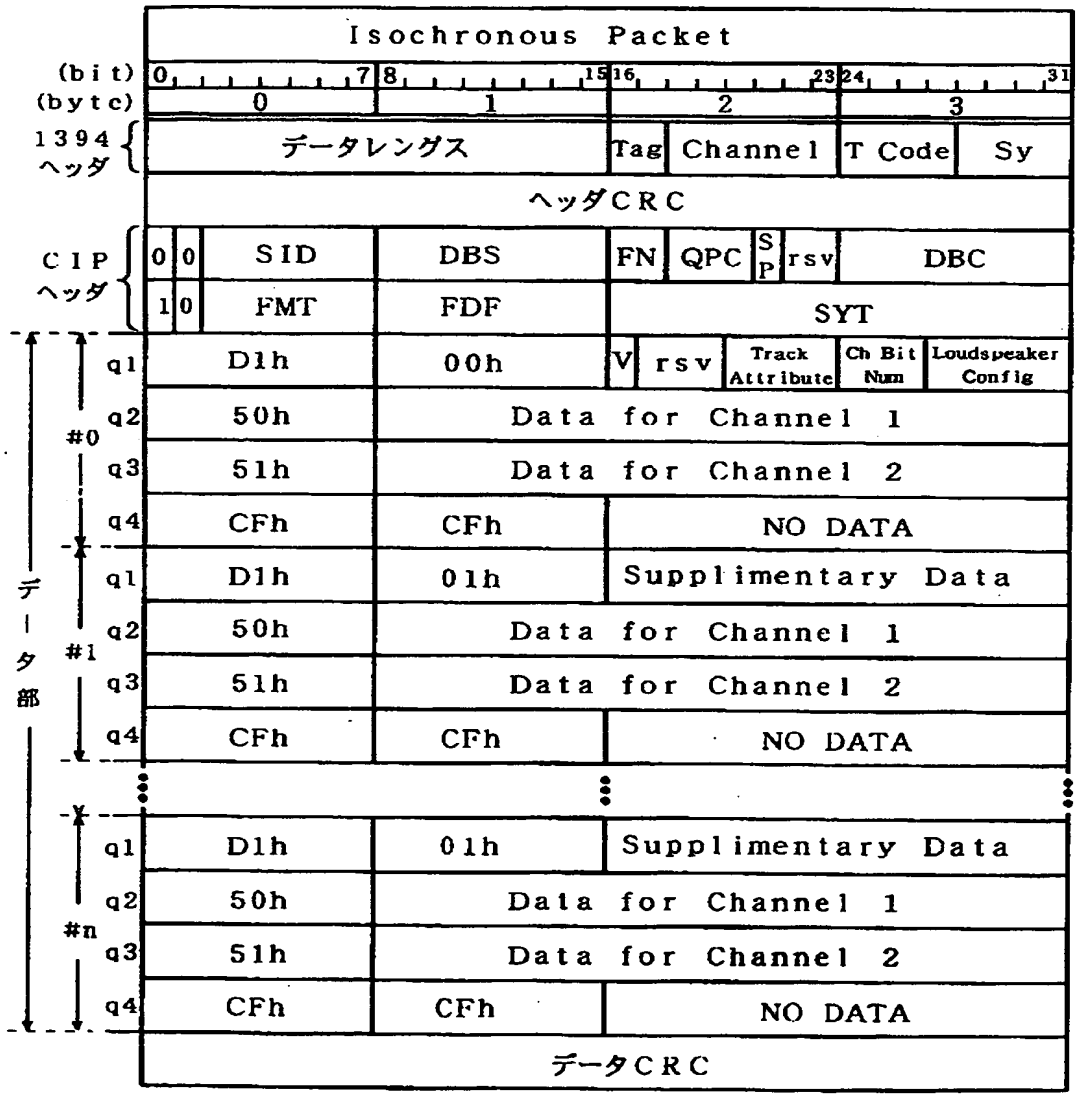
【図２】


(a)
オーディオソース
TRACK#1
TRACK#2
TRACK#3
(b)
トラック#2
無音
音楽
無音
DT
Tad1
Tad2
(c) DTad
ランダムノイズ
無音
音楽
無音
ランダムノイズ
(d) DTs
暗号化ランダムノイズ
暗号化音楽データ
暗号化ランダムノイズ

【図３】


CSP
Asy
Iso
CSP
Asy
Iso
CSP
通信サイクル
通信サイクル
(a)
(b)
アイソクロナスパケット
1394 ヘッダ
ヘッダ CRC
CIPヘッダ
データ部（n個のデータブロック）
データ CRC

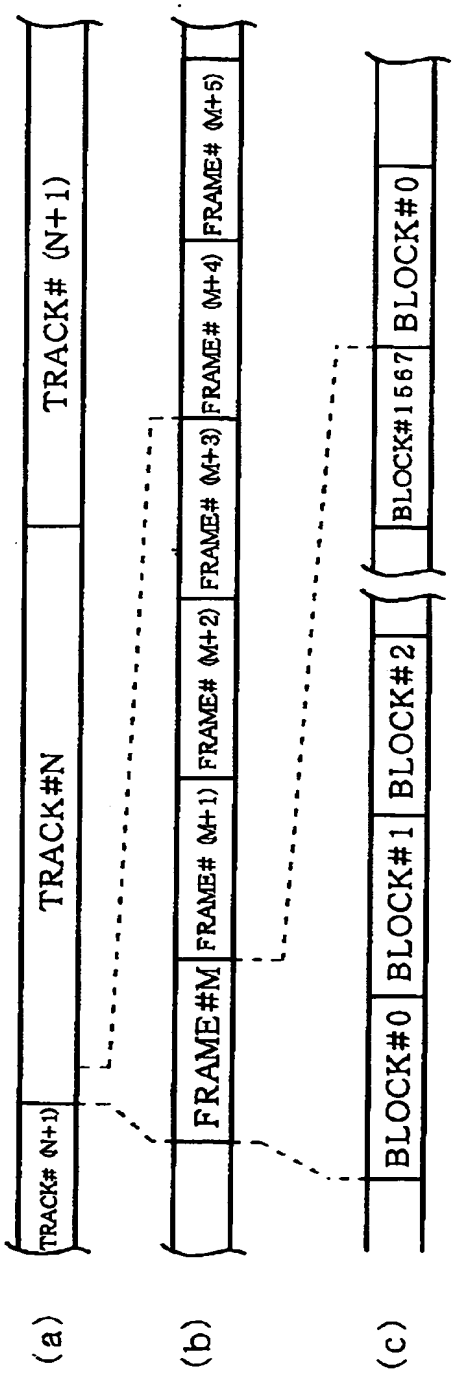
【図４】


Isochronous Packet
(bit)
(byte)
0
7
8
15
16
23
24
31
0
1
2
3
1394 ヘッダ
データレングス
Tag
Channel
T Code
Sy
ヘッダCRC
CIP ヘッダ
0
0
SID
DBS
FN
QPC
SP
rsv
DBC
1
0
FMT
FDF
SYT
データ部
#0
#1
#n
q1
q2
q3
q4
D1h
00h
V
rsv
Track Attribute
Ch Bit Num
Loudspeaker Config
50h
Data for Channel 1
51h
Data for Channel 2
CFh
NO DATA
01h
Supplimentary Data
データCRC

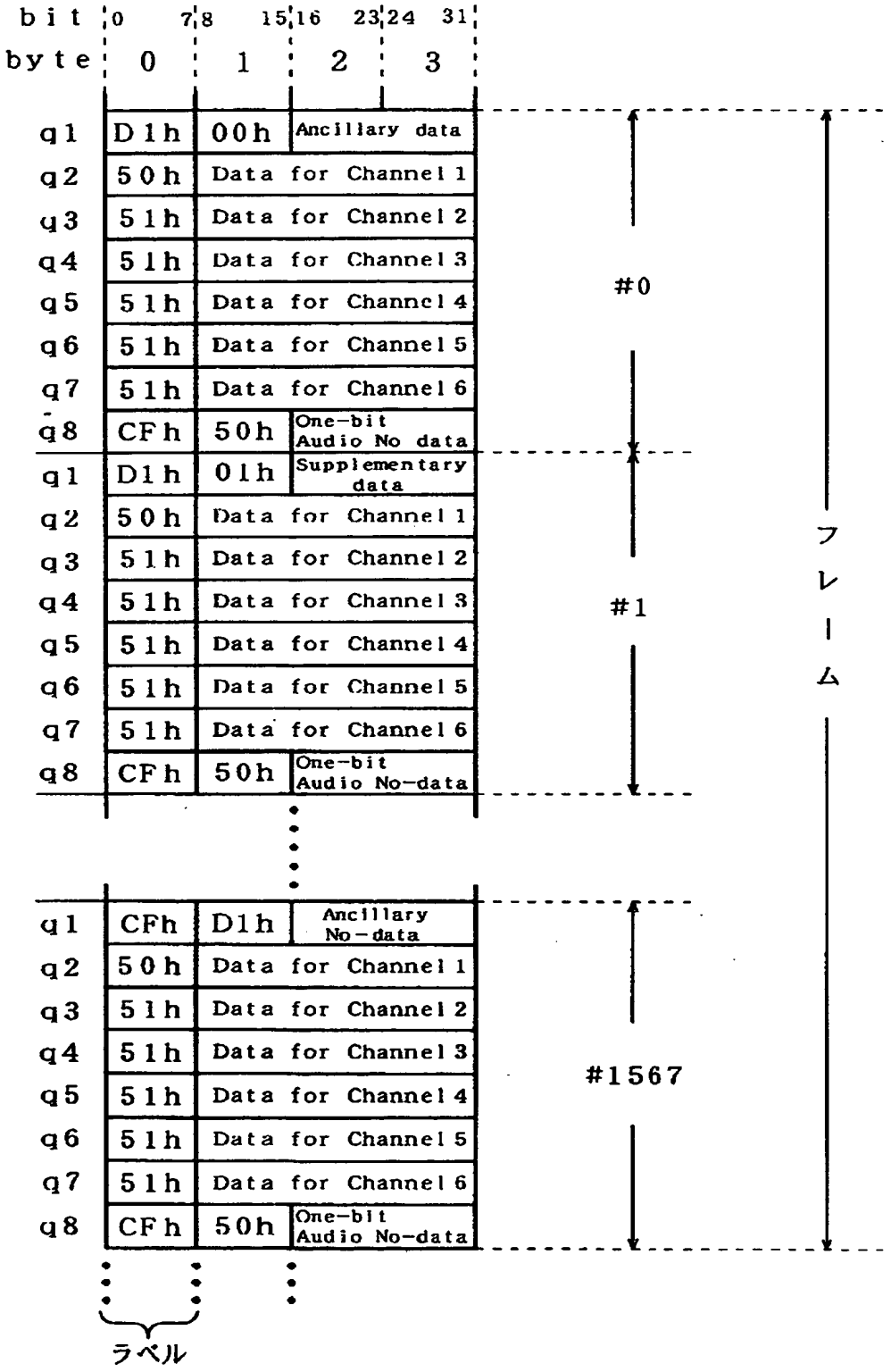
【図５】

Value	Description
00h-3Fh	IEC60958 Conformant
40h-4Fh	Multi-bit Linear Audio
50h-57h	One Bit Audio (Plain)
58h-5Fh	One Bit Audio (Encoded)
60h-7Fh	-reserved-
80h-83h	MIDI Conformant
84h-87h	Extended Music Data
88h-8Bh	SMPTE Time Code Conformant
8Ch-8Fh	Sample Count
90h-BFh	-reserved-
C0h-EFh	Ancillary Data
F0h-FFh	-reserved-

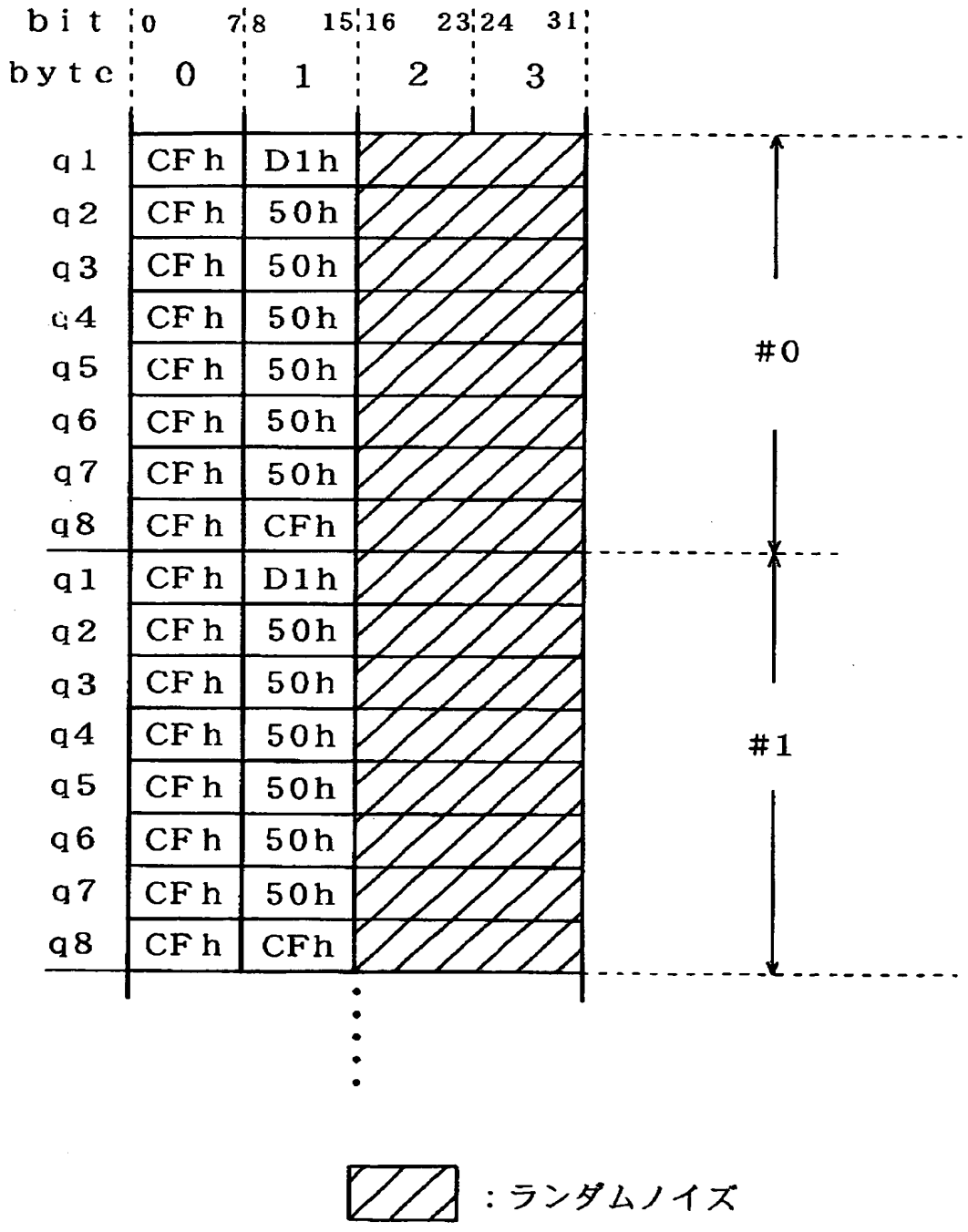
【図６】


TRACK# (N+1)
TRACK#N
FRAME#M
FRAME# (M+1)
FRAME# (M+2)
FRAME# (M+3)
FRAME# (M+4)
FRAME# (M+5)
BLOCK#0
BLOCK#1
BLOCK#2
BLOCK#1567
BLOCK#0
(a)
(b)
(c)

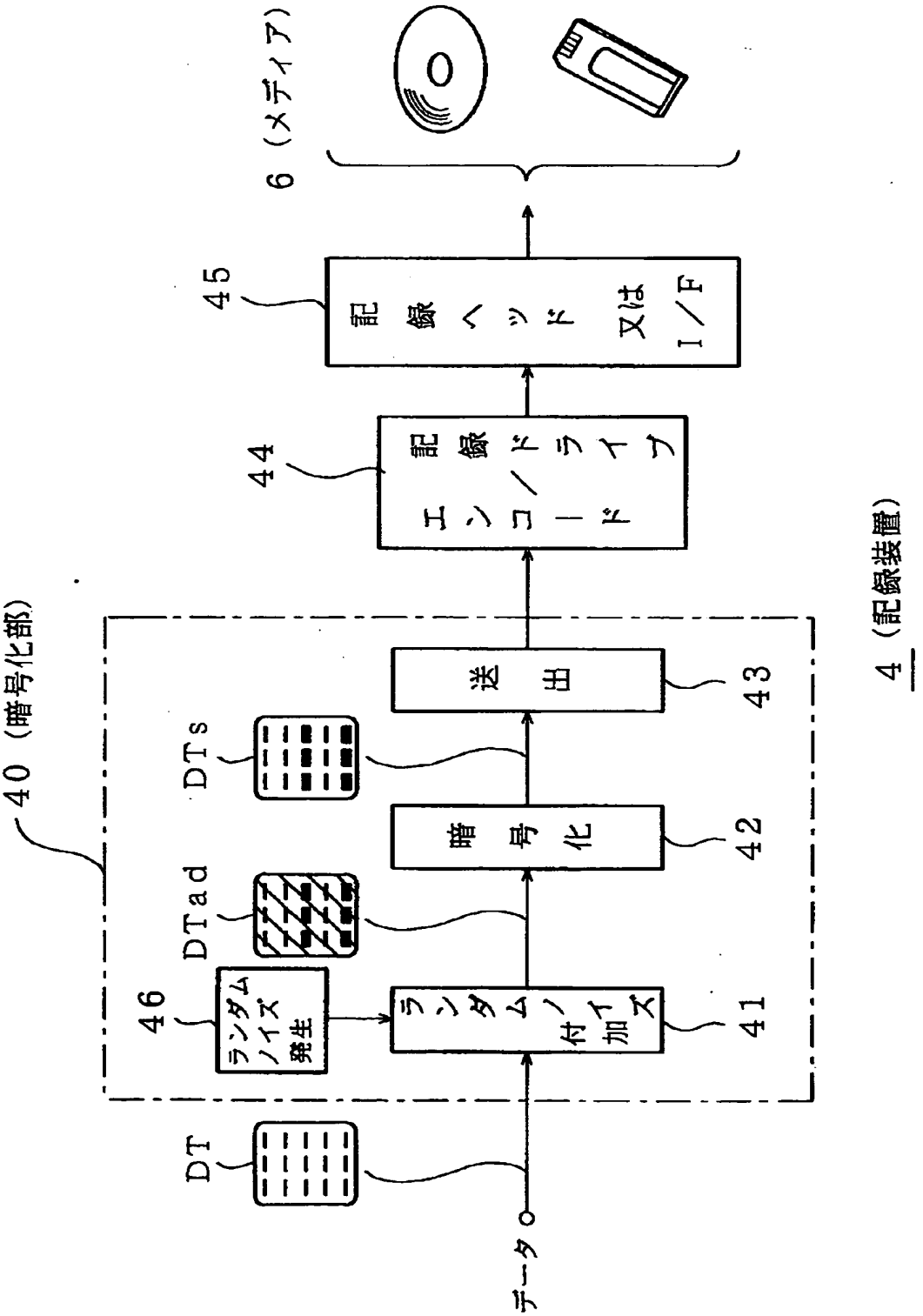
【図７】


bit 0 7 8 15 16 23 24 31
byte 0 1 2 3
q1 D1h 00h Ancillary data
q2 50h Data for Channel 1
q3 51h Data for Channel 2
q4 51h Data for Channel 3
q5 51h Data for Channel 4
q6 51h Data for Channel 5
q7 51h Data for Channel 6
q8 CFh 50h One-bit Audio No data
#0
q1 D1h 01h Supplementary data
q2 50h Data for Channel 1
q3 51h Data for Channel 2
q4 51h Data for Channel 3
q5 51h Data for Channel 4
q6 51h Data for Channel 5
q7 51h Data for Channel 6
q8 CFh 50h One-bit Audio No-data
#1
フレーム
q1 CFh D1h Ancillary No-data
q2 50h Data for Channel 1
q3 51h Data for Channel 2
q4 51h Data for Channel 3
q5 51h Data for Channel 4
q6 51h Data for Channel 5
q7 51h Data for Channel 6
q8 CFh 50h One-bit Audio No-data
#1567
ラベル

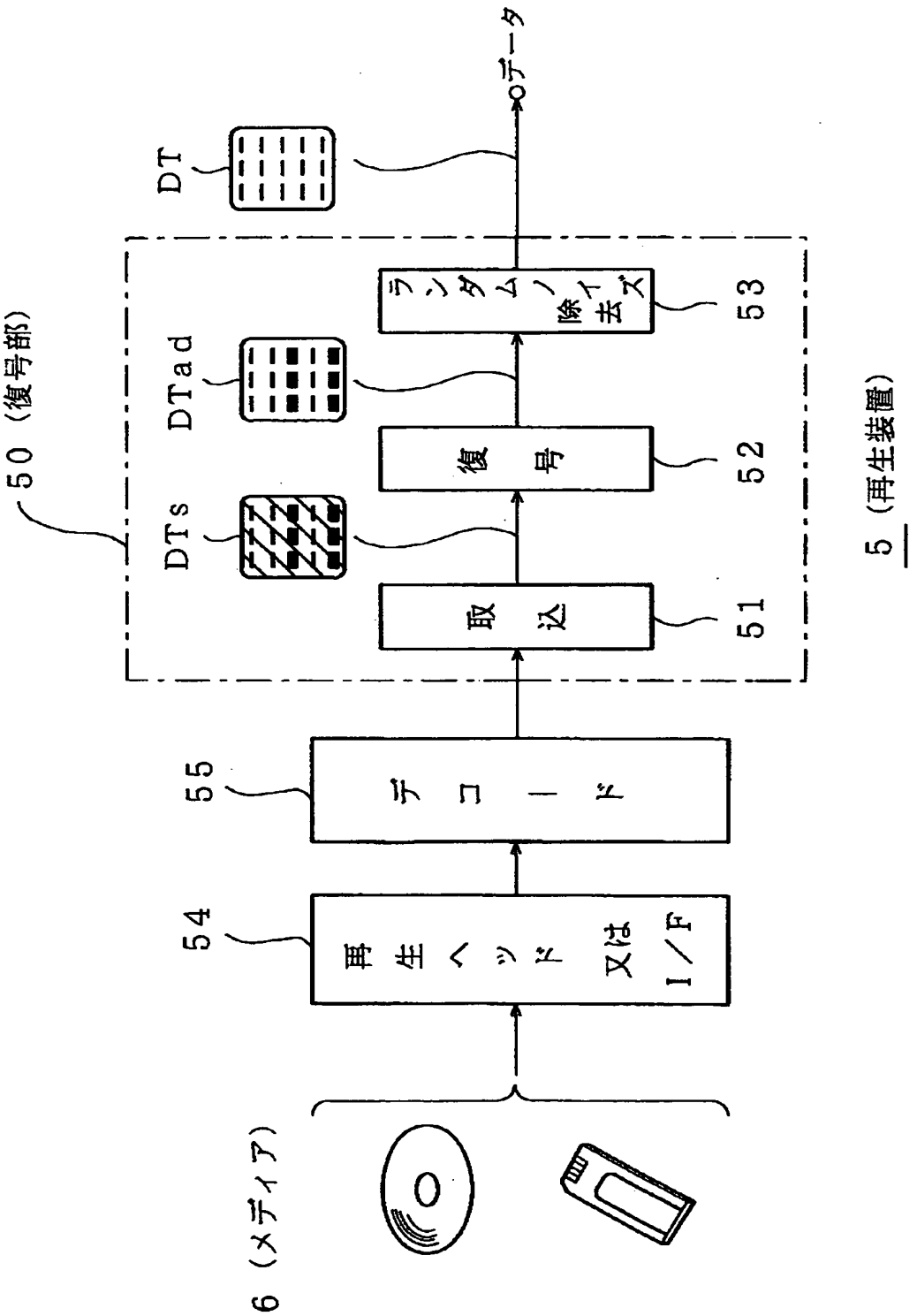
【図８】


bit
0 7 8 15 16 23 24 31
byte
0
1
2
3
q1 CFh D1h
q2 CFh 50h
q3 CFh 50h
q4 CFh 50h
q5 CFh 50h
q6 CFh 50h
q7 CFh 50h
q8 CFh CFh
q1 CFh D1h
q2 CFh 50h
q3 CFh 50h
q4 CFh 50h
q5 CFh 50h
q6 CFh 50h
q7 CFh 50h
q8 CFh CFh
#0
#1
：ランダムノイズ

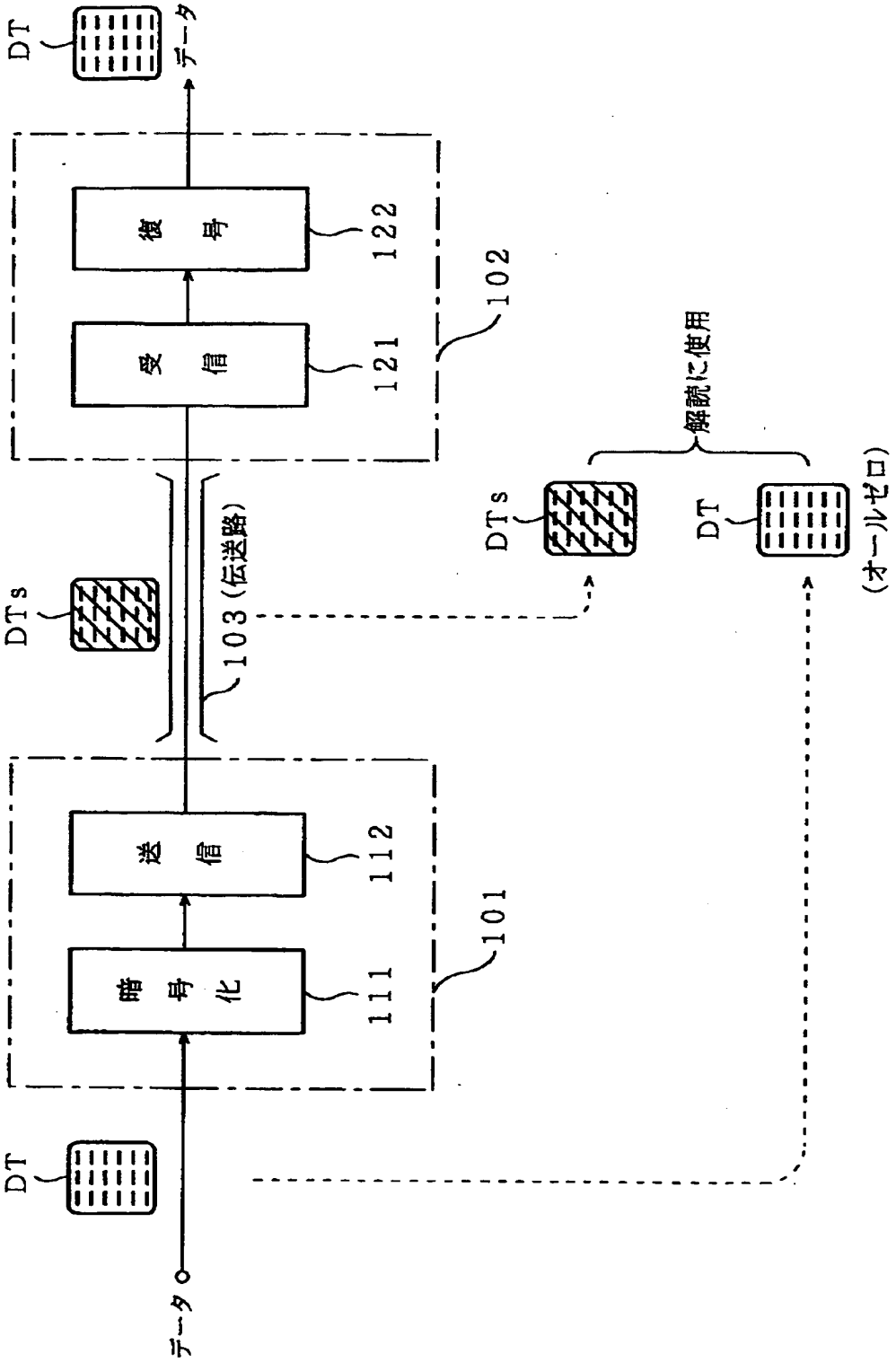
【図９】


6（メディア）
45
記録ヘッド又はI／F
44
記録ドライブエンコード
4（記録装置）
40（暗号化部）
送出
43
DTs
暗号化
42
DTad
46
ランダムノイズ発生
ランダムノイズ付加
41
DT
データ

【図１０】


データ
DT
DTad
DTs
50（復号部）
ランダムノイズ除去
53
復号
52
取込
51
5（再生装置）
55
デコード
54
再生バッファ又はI／F
6（メディア）

【図１１】


DT
データ
復　号
122
受　信
121
102
解読に使用
DTs
DT
(オールゼロ)
DTs
103(伝送路)
送　信
112
暗号化
111
101
DT
データ

【書類名】　　要約書

【要約】

【課題】　暗号解読が困難で著作権保護などに好適なデータ伝送の実現。

【解決手段】　伝送するプログラムデータについて、その前後にランダムノイズを付加したうえで暗号化を行なって伝送し、伝送過程などで暗号化データが抽出されたとしても、暗号アルゴリズムの解読を困難なものとする。データの復号は、暗号化を解読したうえでランダムノイズが付加されたデータ部分を除去することで行う。

【選択図】　　図２

認定・付加情報

特許出願の番号	特願２０００－２６０８６４
受付番号	５００００５０４４２９９
書類名	特許願
担当官	風戸　勝利　　９０８３
作成日	平成１２年　８月３０日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	000002185
【住所又は居所】	東京都品川区北品川６丁目７番３５号
【氏名又は名称】	ソニー株式会社

【代理人】　申請人

【識別番号】	100086841
【住所又は居所】	東京都中央区新川１丁目２７番８号　新川大原ビル６階
【氏名又は名称】	脇　篤夫

【代理人】

【識別番号】	100114122
【住所又は居所】	東京都中央区新川１丁目２７番８号　新川大原ビル６階　脇特許事務所
【氏名又は名称】	鈴木　伸夫

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社